UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/928,491	08/14/2001	Stefan Andersson	027557-061	7917

7590 02/22/2005

Ronald L. Grudziecki
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, VA 22313-1404

EXAMINER	
WILLIAMS, JEFFERY L	
ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 02/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/928,491	ANDERSSON, STEFAN	
	Examiner	Art Unit	
	Williams Jeffery	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-27 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-27 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 14 August 2001 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 12/18/03,2/13/02
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Remarks

Claims 1 – 27 are pending.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 8, 9, 12 – 15, 17 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Regarding claim 8, it is a device claim wherein the language "comprising a cryptographic module" allows the claim to be implemented solely in software (Specification, lines 21, 22). It is therefore rejected under 35 U.S.C. 101 as not being tangible.

Regarding claims 9, 12 – 15, and 17, they are rejected because they do not further include by necessity any hardware in view of claim 8. They are therefore rejected under 35 U.S.C. 101 as not being tangible.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 3, 5, and 6 are rejected under 35 U.S.C. 102(b) as being anticipated by Caputo et al., "Pocket Encrypting and Authenticating Communications Device", U.S. Patent 5,778,071.

Regarding claim 1, Caputo et al. discloses a method of authenticating communications, the method comprising:

using a mobile communications device, which includes a cryptographic module for use in mobile communication, as an authentication token (Caputo et al., Col. 2, lines 23-27; Col. 3, lines 33-38, 46-50).

Regarding claim 3, Caputo et al. discloses:

the use of the mobile communications device as an authentication token includes using public key encryption of communications (Caputo et al., Col. 1, lines 27-39; Col. 11, lines 18-59).

Regarding claim 5, Caputo et al. discloses:

the mobile communications device is used as an authentication token for a computer, and authenticates communications between the computer and an authentication server (Caputo et al., Fig. 3, elem. 38; Fig. 5A, elem. 57; Col. 5, lines 15-20; Col. 13, lines 4-67). The computer or protected communications facility performs the function of an "authentication server" by authenticating the identity of a device/user.

Regarding claim 6, Caputo et al. discloses:

providing a wired connection between the mobile communications device and the computer (Caputo et al., Col. 6, lines 41-61).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2, 4, 8, 9, 12, 14 – 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Caputo et al. as applied to claims 1, 3, 5, and 6 above, further in view of Grimm et al., "Portable Computer Stored Removable Mobile

Telephone", U.S. Patent 5,907,815, and further in view of Geiger et al., "Secure Wireless Electronic-Commerce System with Wireless Network Domain", U.S. Patent 6,463,534 B1.

Caputo et al. discloses a mobile communications device, comprising a cryptographic module, which is used as a token for authenticating a user and for encrypting communications (Caputo et al., Col. 2, lines 23-27; Col. 3, lines 33-38, 46-50; Fig. 2). The device sends communications to a recipient by wired telephonic means (Caputo et al., Fig. 2, elem. 14; Col. 16, lines 40-45; Col. 17, lines 3-7). Caputo et al, however, does not disclose that the device sends the communications by wireless means, or that the device is enabled to use the enhanced wireless security of the Wireless Application Protocol.

Grimm et al. discloses a mobile communications device ("wireless phone") that is enabled to send communications from a user of a connected computer via wireless telephonic means (Grimm et al., Col. 12, lines 12-33; Fig. 7; Fig. 9).

Thus it would have been obvious to one of ordinary skill in the art to combine the wireless mobile communication feature of Grimm et al. with the mobile communication device of Caputo et al. because it is apparent that the ability to operate wirelessly would enhance a communication device designed to be mobile and portable.

Geiger et al., discloses a wireless device and system used to send secure wireless transactions using the Wireless Application Protocol (Geiger et al., Col. 2, lines 49-65; Col. 9, lines 22-53). As disclosed by Geiger et al., WAP is a convenient protocol to use with wireless communications, chosen for its security.

Thus, it would have been obvious to one of ordinary skill in the art to combine the use of the Wireless Application Protocol and system of Geiger et al. with the combination of Caputo et. al. and Grimm et al. because it is obvious that a wireless mobile communication device designed for authenticated and encrypted communications would be enhanced by the use of a communication protocol and system that features increased wireless security.

Regarding claim 2, the combination of Caputo et al., Grimm et al., and Geiger et al., disclose:

the mobile communications device is a WAP-enabled device (Geiger et al., Fig. 1, Col. 9, lines 22-53). As disclosed, the device is WAP-enabled since it communicates using the WAP protocol.

Regarding claim 4, the combination of Caputo et al., Grimm et al., and Geiger et al., disclose:

the mobile communications device uses the cryptographic module for Wireless Transport Layer Security communications (Geiger et al., Col. 2, lines 49-65; Col. 6, lines 55-58; Col. 9, lines 22-53). As disclosed, communication security, the functionality provided by the cryptographic module, is accomplished using WTLS communications.

Regarding claim 8, the combination of Caputo et al., Grimm et al., and Geiger et al., disclose a mobile communications device, comprising a cryptographic module, the cryptographic module being useable:

for encoding wireless communications from the device (Caputo et al., Col. 2, lines 23-27);

for authenticating a user of the device towards an authentication server (Caputo et al., Fig. 3, elem. 38; Fig. 5A, elem. 57; Col. 5, lines 15-20; Col. 13, lines 4-67). The computer or protected communications facility performs the function of an "authentication server" by authenticating the identity of a device/user.

Regarding claim 9, the combination of Caputo et al., Grimm et al., and Geiger et al. disclose *the cryptographic module being usable for authenticating a user of a separate computer towards an authentication server* (Caputo et al., Fig. 3, elems. 22, 38; Fig. 5A, elem. 57; Col. 5, lines 15-20; Col. 13, lines 4-67). The computer or protected communications facility performs the function of an "authentication server" by authenticating the identity of a device/user.

Regarding claim 12, the combination of Caputo et al., Grimm et al., and Geiger et al. disclose *the cryptographic module is usable to support wireless communications using Wireless Transport Layer Security* (Geiger et al., Col. 2, lines 49-65; Col. 6, lines 55-58; Col. 9, lines 22-53). As disclosed, communication security, the functionality provided by the cryptographic module, is accomplished using WTLS communications.

Regarding claim 14, the combination of Caputo et al., Grimm et al., and Geiger et al. disclose *the cryptographic module uses public key cryptography* (Caputo et al., Col. 1, lines 27-39; Col. 11, lines 18-59).

Regarding claim 15, the combination of Caputo et al., Grimm et al., and Geiger et al. disclose *means for sending and transmitting data using WAP* (Geiger et al., Fig. 1, Col. 9, lines 22-53). As disclosed, the device is WAP-enabled since it communicates using the WAP protocol.

Regarding claim 16, the combination of Caputo et al., Grimm et al., and Geiger et al. disclose *the cryptographic module is realized in hardware in the device* (Caputo et. al., Col. 8, lines 34-55; Col. 9, lines 28-45). As disclosed, the cryptographic module, the cryptographic component(s), may be either software or hardware.

Regarding claim 17, the combination of Caputo et al., Grimm et al., and Geiger et al. disclose *the cryptographic module is realized in software in the device* (Caputo et. al., Col. 8, lines 34-55; Col. 9, lines 28-45). As disclosed, the cryptographic module, the cryptographic component(s), may be either software or hardware.

Regarding claim 18, the combination of Caputo et al., Grimm et al., and Geiger et al. disclose *the cryptographic module is provided on an external smart card* (Caputo et. al., Col. 10, lines 19-31, 51-59; Col. 13, lines 4-10, 25-67). As disclosed, the

cryptographic module, the cryptographic component(s), may be provided on an external smart card.

Regarding claim 19, the combination of Caputo et al., Grimm et al., and Geiger et al. disclose *the cryptographic module comprises a Wireless Identity Module (WIM) card* (Geiger et. al., Col. 11, line 64 – Col. 12, line 8). As disclosed, the cryptographic module, the cryptographic/authentication component(s), may comprise a WIM card.

Regarding claim 20, the combination of Caputo et al., Grimm et al., and Geiger et al. disclose *the cryptographic module comprises a Wireless Identity Module (WIM) card which allows communications using Wireless Transport Layer Security* (Geiger et. al., Col. 11, line 64 – Col. 12, line 8). As disclosed, the WIM card provides an interface for using the WAP security layer (WTLS).

Regarding claim 21, it is rejected for the same reasons as claims 1 and 2.

Regarding claim 22, the combination of Caputo et al., Grimm et al., and Geiger et al. disclose a communications network, comprising:

at least one WAP gateway, which is enabled to encrypt communications on the basis of Wireless Transport Layer Security (Geiger et al., Figs. 1, 4; Col. 6, lines 49-64; Col. 9, lines 21-53);

at least one authentication server operable in a first authentication protocol (Caputo et al., Fig. 3, elem. 38; Fig. 5A, elem. 57; Col. 5, lines 15-20; Col. 13, lines 4-67). The computer or protected communications facility performs the function of an "authentication server" by authenticating the identity of a device/user.

a WAP-enabled client device, including a cryptographic module, the cryptographic module being usable for encrypting communications with the WAP gateway using the Wireless Transport Layer Security, and the cryptographic module being further usable as an authentication token for authenticating a user of the device towards the authentication server, using the first authentication protocol (Geiger et al., Col. 2, lines 49-65; Col. 6, lines 55-58; Col. 9, lines 22-53; Col. 2, lines 23-27; Col. 3, lines 33-38, 46-50). As disclosed, encrypted communications, functionally provided by the cryptographic module, are accomplished by the device using WTLS. Furthermore, the device is used as a token for authenticating a user of the device towards a authentication server.

Regarding claims 23 – 26, they are system claims related to device claims 16 – 19, and are rejected for the same reasons.

Regarding claim 27, it is rejected for the same reasons as claims 1, 2, 5, and 22.

Claims 7, 10, and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Caputo et al., Grimm et al., and Geiger et al. as applied to claims 1 – 6, 8, 9, 12, and 14 – 27 above, further in view of Ericsson, "Bluetooth – A Global Specification for Wireless Connectivity".

Regarding claims 7, 10, and 11, the combination of Caputo et al., Grimm et al., and Geiger et al. disclose a wired connection between the device and the computer (Caputo et al., Col. 6, lines 41-61). They do not disclose a wireless connection or connection via a short-range transceiver incorporating Bluetooth wireless technology.

Ericsson discloses the obvious use of wireless connections between devices (Ericsson, Page 1). Bluetooth, a short-range radio technology allows for the replacement of wired connections – "facilitating protected" wireless connections between mobile devices. As disclosed, Bluetooth technology can be used to replace "the cumbersome cable used today to connect a laptop to a cellular telephone".

It would be obvious to one of ordinary skill in the art to combine the secure feature of wireless short-range radio connection and Bluetooth technology of Ericsson with the combination of Caputo et al., Grimm et al., and Geiger et al. because it is apparent that the ability to securely operate wirelessly would enhance a security/communication device designed to be mobile and portable.

Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Caputo et al., Grimm et al., and Geiger et al. as applied to claims 1 – 6, 8, 9, 12, and 14 – 27 above, further in view of Gullman et al., "Biometric Token For Authorizing Access to a Host System".

Regarding claim 13, the combination of Caputo et al., Grimm et al., and Geiger et al. disclose a mobile communications device that is used as a token. Also disclosed, is that biometric information may be used to identify a user (Caputo et al., Col. 1, lines 45-67). However, it does not disclose specifically that a mobile communications device could have means for allowing the biometric identification of a user.

Gullman et al., describes a mobile communications device having means for allowing the biometric identification of a user (Gullman et al., Col. 2, lines 48-65). Gullman et al. discloses that the additional means for allowing the biometric identification of a user, increases the security of a key-based token.

It would have been obvious to one of ordinary skill in the art to combine the means for allowing the biometric identification of Gullman et al. with the mobile communications device of Caputo et al., Grimm et al., and Geiger et al. because it is obvious that a device designed securely authenticate a user would be enhanced by more secure methods of authentication.

Claims 1 – 27 are rejected under 35 U.S.C. 102(a) as being unpatentable over Nordman, "Secure Access Method, and Associated Apparatus, for Accessing a Private IP Network", U.S. Patent 6,061,346.

Regarding claims 1 – 27, they are rejected for the reasons provided in the International Search Report (HL76382/004/KM) on 11/9/2001 in response to application no. PCT/EP 01/08320.

Conclusion

The following prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Seiderman, "Portable Cellular Telephone With Credit Card Debit System", U.S. Patent 5,850,599.

b. Wang, "Portable Electronic Authorization Devices and Methods Therefor", U.S. Patent 5,917,913.

c. Muftic, "Smart Token System for Secure Electronic Transactions and Identification", U.S. Patent 5,943,423.

d. Muftic, "Secure World Wide Electronic Commerce Over an Open Network", U.S. Patent 5,850,442.

d. "WAP White Paper", AU-System, February 1999.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Williams Jeffery whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Caldwell Andrew can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at (866) 217-9197 (toll-free).

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER